

Information System Administrator Operations and Security Training

Recommended Approaches to Training,
Educating, and Licensing Department of
Defense Systems Administrators

January 9, 1998

Table of Contents

TABLE OF CONTENTS.....	II
PURPOSE.....	3
INTRODUCTION.....	3
SYSTEM ADMINISTRATOR LEVELS.....	4
LEVEL 1.....	5
<i>Skills</i>	5
<i>Tasks</i>	5
<i>Goals</i>	5
LEVEL 2.....	6
<i>Skills</i>	6
<i>Tasks</i>	6
<i>Goals</i>	7
LEVEL 3.....	7
<i>Skills</i>	7
<i>Tasks</i>	8
LEVEL RECOGNITION.....	8
APPENDIX A	ERROR! BOOKMARK NOT DEFINED.
APPENDIX B	ERROR! BOOKMARK NOT DEFINED.
APPENDIX C	ERROR! BOOKMARK NOT DEFINED.

Purpose

It is imperative that the Department of Defense (DoD) understands and manages today's dynamic and growing information system processing infrastructure. Through various programs and policies, there is an inordinate number of people performing tasks as *system administrators*. Some of these tasks can be performed with little knowledge while others require extensive experience. Results from the *Eligible Receiver* exercise revealed the need to assure consistent verifiable skill sets for individuals functioning as system administrators, primarily in support system security functions. This paper outlines three separate levels and maps skills against them so DoD managers can adequately train system administration personnel, thereby gaining more efficient operational use of them and assuring information system protection.

Introduction

Throughout this paper the term *system administrator* will be used. Services and agencies have various definitions of system administrator, but in all cases systems administrators are generalists. They install, tune, and maintain information systems and associated networks. System administrators:

- teach users operational duties and solve related problems,
- write scripts/programs,
- repair or upgrade hardware,
- with Information System Security Officers, enforce security.

Systems administrators keep an information system environment up and running for their users.

Before continuing, there must be some preliminary clarifications.

1. *Operating system*. Even though a vast majority of system administrators work with UNIX or Windows NT, this guideline is not operating system specific. System administrators are expected to have some experience with the operating system used. These standards can be applied to system administrators of all operating systems.
2. *Education*. A college degree is not required at any level, but formal education is essential for a system administrator. The understanding needed to be able to debug complex problems, tune performance, as well as understanding how operating systems and networks work must come from formal education, re-enforced with on-the-job training. System administrators must have the background that allows

them to recognize *why* solutions work. The DoD should not be in the business of competing with private industry in these areas, but supplementing training provided by academia and private training companies.

3. *Programming*. Programming experience is required beyond the first level. Knowledge of a command language is mandatory to automate tasks and modify system parameters. Knowledge of an appropriate high level language is also important since system administrators should be able to compile source code and debug simple problems. System administration is not for people who do not want to program and it is unlikely that these individuals will progress beyond level 2.

4. *INFOSEC*. Information System Security functions are primarily the responsibility of the Information System Security Officer (ISSO). With dwindling resources and ever decreasing manpower, oftentimes the job of the system administrator and the ISSO blend into one. The INFOSEC functions of a system administrator are:¹

- working closely with the ISSO to ensure the information system or network is used securely,
- participating in the INFOSEC incident reporting program,
- assisting the ISSO in maintaining configuration control of the systems and application software,
- advising the ISSO of security anomalies or integrity loopholes, and
- administering, when applicable, user identification or authentication mechanisms of the information system or network.

System administrator levels

The term *level* in this section was chosen over other semantics for its simplicity and relation to skill levels used by the uniformed services. The break down of levels and tasks does not take into account the practice of specialization. In many organizations, systems administrators gravitate to becoming local experts in a specific topic (e.g., word processing, presentation applications, routers, and e-mail applications), often with no more experience than a Level 1 system administrator.

The term *domain* is used as a way to bound the focus, or realm of control, of any given information system management organization, regardless of the organization size.

¹ NTISSI 4013, National Training Standard for System Administrators in INFOSEC, August 1997, pg. 2.

Level 1

A level 1 system administrator has been working in the field for a while, but is relatively inexperienced. Individuals coming from training organizations or recently graduating from service schools is considered a *trainee* and would reach level 1 status after a predetermined time of on-the-job training, but not normally sooner than one year on the job.²

A healthy domain should have a steady supply of level 1 system administrators progressing to level 2.³

Skills

Level 1 skills should include:

- at least one year of experience administrating the relevant operating system,
- formal training for the operating system and command language,
- strong customer relation skills.

Tasks

Level 1 tasks should include:

- day-today operations such as backups, restores, adding/modify/deleting user accounts
- installing operating systems, applications and peripherals
- troubleshooting user problems
- debugging command language scripts
- assisting the ISSO in access control security (i.e., passwords, etc.)

Goals

Level 1 advancement goals should include:

- learning why a solution works, not just how to implement it
- obtaining formal training in core computer science and system courses
- obtaining formal training in organization or domain specific courses

² By this time they should be solving more problems than they create. If other system administrators are spending more time helping and training the individual than spending on system tasks, then the individual is still a trainee.

³ If the level 1's are ever in the majority, the domain runs the risk of burning out the level 2 and level 3 system administrators.

Level 2

Level 2 systems administrators are the work-horses in a domain. They perform the majority of the daily tasks that keep a domain running smoothly. They are the expert jugglers that can work simultaneously on several problems. The ultimate success of a domain is highly dependent on having a core group of level 2 system administrators. At least half of the system administrators in a healthy domain should be at level 2.

Skills

Level 2 skills should include:

- at least 3 years of experience in administrating the relevant operating system
- formal training in networking, programming language concepts & algorithms
- formal training in firewall management and telecommunication fundamentals
- knowledge of all interactions within their domain
- ability to program in a command language
- ability to spot redundant tasks and automate them
- strong communications skills. can explain solutions for complex problems to users and other system administrators
- independently solving non-trivial problems
- working in groups with other system administrators to jointly solve problems
- with the ISSO, ability to successfully implement security mechanisms on networks and systems within their domain

Tasks

Level 2 tasks should include:

- taking the lead in solving day-to-day operational problems
- implementing complex operating system changes
- with the ISSO, ensuring that established security mechanisms are functioning properly
- debugging operating system, application, and network problems
- following domain parameters, defining default environment for systems for users
- maintain and enforce adherence to standards
- monitor and balance load among servers and networks within the domain
- interacting with developers, operations centers, and support personnel to maintain daily operations
- keeping the environment up and running smoothly

Goals

Level 2 advancement goals should include:

- obtaining formal training in core computer science & system courses
- sharing knowledge with system administration community by publishing articles, teaching, acting as a mentor, and participating in conferences
- participating in special focus groups

Level 3

The most experienced administrators are few and far between. They have successfully separated themselves from the daily operations and concentrate on tasks that can be leveraged with their knowledge. Large domains should have one or two level 3 administrators leading the technical effort and setting the policy and direction for the domain. The absence of a level 3 will tend to leave the domain with no clear direction.⁴

Skills

Level 3 skills should include:

- At least 5 years or more of extensive experience administering the relevant operating system
- Formal training in at least the following core computer science courses
 - Operating System Design
 - Data/Algorithm Structure
 - Machine Architecture
 - Networking
 - Programming Language Concepts/Algorithms
- A strategic view of the domain operation/mission, and interaction with all external domains
- Fluency in at least one command language
- Experience with applicable programming languages
- Ability to work independently to quickly and completely solve problems
- Ability to lead a team to quickly and completely solve problems
- Strong interpersonal, organizational, and communication skills. Can make presentations, write proposals, and interact with management and other organizations
- Ability to train junior system administrators

⁴ Too many level 3 system administrators will tend to produce either a committee approach or head-butting contest. In either case there will not be a consistent direction for the domain.

Tasks

Level 3 tasks should include:⁵

- Taking general direction from management and turning it into a well thought out solution or design
- Setting and/or interpreting standards
- Planning and designing the architecture of their domain
- Working with the ISSM and ISSOs, planning security procedures, mechanisms, and architecture of their domain
- Tuning the performance of existing domains
- Solving the tough problems that others have not been able to fix
- Leading teams to tackle complex problems
- Teaching other system administrators
- Publishing guidance and lessons learned

Level Recognition

The requirements outlined at each level are rather subjective. Services and agencies do not need another set of standards to meet, in addition to current regulations and policies in place. Level recognition can be loosely based on an individual's status within existing information system career panel organizations. Appendix A draws from the National Security Agency System Administration Specialty Job Task Analysis Map⁶ and cross-references recommended levels to job tasks. These tasks can be supplemented by standards listed in NTISSI 4013 and NTISSI 4014⁷. Appendix B draws from standards listed in the draft replacement to NIST Special Publication 500-172⁸ Appendix C draws from discussions with US Army and US Navy trainers.⁹

⁵ Nothing relating to Level 1 tasks. Lose the screwdriver!

⁶ NSA Computer System Manager System Administration Specialty (CSM-SA), July 1996

⁷ National Training Standard for Information Systems Security Officers (ISSO), August 1997

⁸ Information Technology Security Training Requirements: A Role- and Performance-Based Model, December 1997

⁹ DISA meeting with Navy trainers in Pensacola FL, Sept 97; with Army trainers in Ft. Gordon GA, Oct 97